
Article:
Monkhouse, Helen, Habli, Ibrahim orcid.org/0000-0003-2736-8238 and McDermid, John Alexander orcid.org/0000-0003-4745-4272 (2020) An Enhanced Vehicle Control Model for Highly Automated Driving Safety. Reliability Engineering and System Safety. pp. 1-12. ISSN 0951-8320

https://doi.org/10.1016/j.ress.2020.107061

An Enhanced Vehicle Control Model for Assessing Highly Automated Driving Safety

Helen E Monkhouse[a,*], Ibrahim Habli[b], John McDermid[b]

[a]*HORIBA MIRA Ltd., Watling Street, Nuneaton, CV10 0TU, UK*
[b]*High Integrity Systems Engineering, Department of Computer Science, University of York, Deramore Lane, University of York, Heslington, York, YO10 5GH, UK*

Abstract

Automation has been changing the types and causes of hazards, and influencing the way in which users interact with complex systems, particularly challenging the notion of human control as a primary basis for hazard mitigation. In this paper, we explore this challenge and use an automotive driving example to examine the distributed nature of the driving task.

We define an Enhanced Vehicle Control Model (VCM) that extends the notion of controllability and joint cognition for highly automated tasks. We apply the model to three contemporary driver assistance systems by undertaking a scenario-based evaluation. As a conceptual model, the Enhanced VCM shows potential to proactively identify the hazard causes associated with a joint cognitive control. However, to provide utility and to become an effective tool for the system analyst, an accompanying methodology is needed.

Keywords: automated driving, functional safety, SOTIF, vehicle control model, hazard analysis, joint cognitive system (JCS)

1. Introduction

Embedded electronic control systems first appeared in passenger vehicles in the 1980's and were introduced to replace specific mechanical engine con-

*Corresponding author

Email addresses: helen.monkhouse@horiba-mira.com (Helen E Monkhouse), ibrahim.habli@york.ac.uk (Ibrahim Habli), john.mcdermid@york.ac.uk (John McDermid)

trols (e.g. electronic ignition, fuel injection). However, the need for greater efficiency and the introduction of more stringent emissions targets, meant that within a decade everything from driver demand to air and fuel mix were under the control of embedded programmable electronics. The proliferation of such systems raised concerns about the impact that a control system failure might have on vehicle safety. To address these concerns the UK government set up the Motor Industry Software Reliability Association (MISRA) consortium in the early 1990's, with the objective being to *"provide assistance to the automotive industry in the creation and application within a vehicle system of safe, reliable software"*. The "MISRA Guidelines" [1] provided the practising engineer with guidance describing the activities necessary to evaluate the safety implications of programmable automotive systems, and to achieve *functional safety*; that is, the absence of unreasonable risk caused by embedded electronics hardware and software faults. This included a method for assessing risk (the MISRA Risk Model) that considered the effects of failure on system behaviour (the hazards) and used, amongst other things, the concept of controllability (i.e. the ability of the persons in harm's way to make the correct and timely reaction to avoid the harm) to estimate the degree of risk associated with vehicle hazards.

When used to classify moving vehicle hazards, the concept of controllability has to date made the assumption that the vehicle driver is a part of the control loop (Figure 1), and given that they are integral to control they are always situationally aware. The introduction of evermore complex Advanced Driver Assistance Systems (ADAS) and the move towards Highly Automated Driving (HAD) changes this assumption. Not only is the driver's role and behaviour potentially changing [2–4], but also vehicles are becoming part of a socio-technical transport system of systems; with the vehicle potentially modifying its behaviour as a result of information received from other vehicles, from roadside infrastructure, and from the Cloud.

Although having the potential to solve many of today's automotive related transport issues, and contributing to WHO's targets[1], the introduction of highly automated and self-driving vehicles is not without its challenges.

[1]The World Health Organization (WHO) estimates that more than 1.25 million people die each year as a result of road traffic accidents and nearly half of those are vulnerable road users; i.e. pedestrians, cyclists and motorcyclists. . The 2030 Agenda for Sustainable Development includes *halving the global number of deaths and injuries caused by road accidents by 2020* [6].

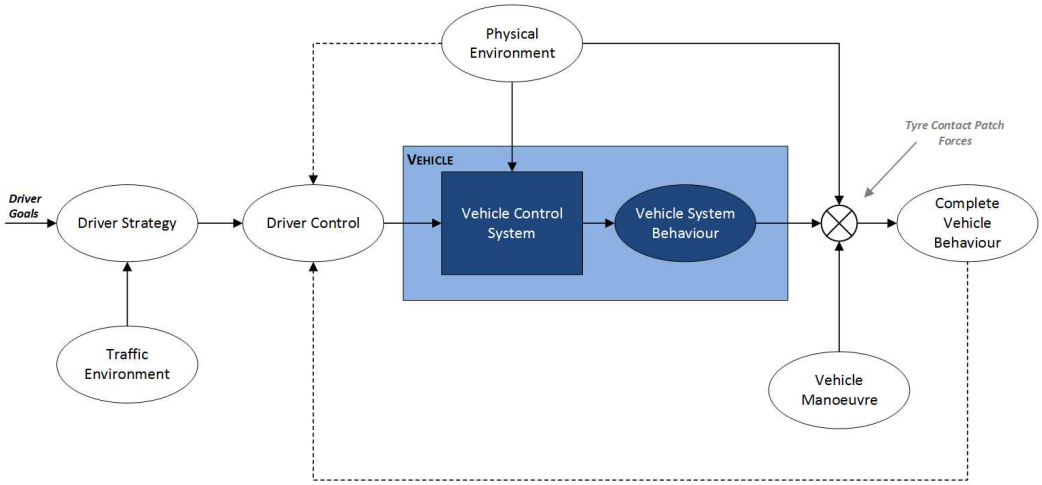

Figure 1: MISRA Control System View of the Vehicle [5]

The public will need assurances that such technology is safe[2] and worthy of their trust [7], legislators will need to adapt the whole-vehicle regulatory framework upon which the technology is released into the market place, while engineers will need to develop new methods to assess, validate and assure the safety of such systems [8].

Typically the risk of hazards associated with fitting a new feature to the vehicle is assessed using the ISO 26262 risk model that assumes the driver is integral to vehicle control. The scope of ISO 26262 is also limited to hazards caused by the malfunctioning behaviour of electrical/electronic (E/E) systems installed in series production vehicles. In 2019 the International Organization for Standardization (ISO) published a Publicly Available Specification (PAS), entitled *Safety Of The Intended Functionality (SOTIF)*, which gives guidance on the development of systems whose Situational Awareness (SA) is critical to safety. Although the SOTIF PAS could potentially be applied to highly automated vehicle systems, its scope is the lower automation levels that require the driver to remain vigilant and responsible for

[2]Research suggests that if safety levels for self-driving technologies were comparable to that of the human driver the general public would deem the risk *unacceptable*, whereas a 4 or 5 times safety improvement would be deemed *tolerable*. However, to be deemed *broadly acceptable* the perceived risk would need to be hundreds of times better than today's accident statistics indicate [7]!

vehicle safety. Examples include Adaptive Cruise Control (ACC), an SAE Level 1 system [9] that automates longitudinal control, and ACC with Lane Centring Assist, an SAE Level 2 system [9] that automates both lateral and longitudinal control.

The first step in the SOTIF process is to identify any potential sources of harm. That is, to identify the triggering events that could lead to hazards and to evaluate the hazard risk. The process suggests prior knowledge and field data as possible means of identifying triggering events [10], while for risk classification the ISO 26262 risk schema is proposed [11]. This approach still requires the automotive safety analyst to conduct *thought experiments* to identify likely hazards and to reason about hazard risk. However, with outcomes being influenced by the vehicle's environment and the shared nature of the driving task, reasoning about hazard risk becomes more complex.

1.1. Research Contribution

Our research aim is to produce a new basis from which to analyse the hazard risk of HAD vehicle features. With our objective being to create a suitable conceptual VCM and method that supports hazard analysis in a HAD context. By including elements representing the shared cognitive nature of the driving task, our research seeks to support the identification of hazards and hazard causes not explored by contemporary hazard models. This contributes a new dimension to automotive hazard analysis not covered by the current automotive safety standards [10, 11] and extends the notion of controllability and joint cognition for highly automated tasks, such as driving.

This paper is the first part of a package of work, that focuses on the development of the Enhanced VCM. In Section 2 we review the literature that has informed the enhancements made to the original MISRA VCM before describing the model itself in Section 3. Then in Section 4 we introduce three HAD vehicle features, which we use to explore the potential utility of our enhanced model. For example, can we describe each HAD features using the model, and does the model highlight how contemporary approaches to hazard, risk and controllability might need to change? Also, for HAD vehicle features that require the Dynamic Driving Task (DDT), and hence vehicle safety, to be shared between the human and the machine, is the model useful in identifying hazard causes that exist because the DDT is shared?

2. Literature Review

2.1. The Functional Safety Paradigm and What Needs to Change

The 'Vienna Convention' [12] requires that *every moving vehicle shall have a driver* and that *every driver shall at all times be able to control his vehicle or to guide his animals*. This gives rise to the implicit automotive functional safety assumptions that: the driver is integral to vehicle control, they will be situationally aware, and given that not every hazardous situation on the road leads to an accident, the driver is often able to control the situation and prevent an accident occurring. The driver's intrinsic role in vehicle control is evident in the MISRA Control System View of the Vehicle (Figure 1).

Definition 1. The ISO 26262 automotive risk matrix [11] describes Risk (R) as:

$$R = F(f, C, S)$$

where F is a function with parameters f representing the frequency of occurrence of a hazardous event, C the controllability , and S the severity of the resulting harm.

By including a *Controllability* parameter the ISO 26262 risk matrix allows credit to be taken for the ability the driver has to control the hazardous situation[3]. However, human factors research suggests that automation will potentially influence *Controllability* by impacting a driver's ability to identify hazards [13], to react, to re-engage appropriately, [14] and to remain situationally aware [15].

The current automotive functional safety paradigm is appropriate to 1990's embedded control systems, whose functionality and interfaces can be easily defined and bounded, and that hold the driver ultimately responsible for vehicle safety [8]. In what ISO 26262 defines as the 'Item' the cause of a hazard will be a hardware or systematic fault within the Item, with the most appropriate mitigation action often being to simply disable the faulty function until it is repaired. In defining its scope as *"is intended to be applied*

[3]with controllability being rated from C0 for *controllable in general* to C4 for *difficult to control or uncontrollable* [11]

to functions where proper system situational awareness is critical to safety, and where that situational awareness is derived from complex sensors and processing algorithms" the SOTIF PAS [10] acknowledges that the safety of today's HAD systems cannot be achieved by simply drawing a boundary around a system and analysing what lies within. To compound the problem the system is no longer the Item or even the vehicle, but instead a complex system of systems, with the vehicle system potentially interacting with other systems, the infrastructure and the Cloud.

When considered in the context of the automotive risk matrix, the MISRA VCM (Figure 1) is useful in *thought experiments* which reason about vehicle behaviour, driver behaviour and automotive risk [16]. Although intended to represent manual driving, many elements of the model remains relevant today, and will remain relevant while vehicles continue to have driver controls. However, for the MISRA VCM to remain a useful model for hazard analysis it needs to: allow automation's influence to be considered, represent the shared nature of the *Driver Control* task, and reflect the human / machine interactions that are pertinent to safety. The MISRA VCM is also drawn from the perspective of a single vehicle. To maintain its usefulness the model needs to represent information coming to the *ego vehicle*[4] from external sources (e.g. other vehicles, roadside infrastructure, the Cloud) and help the analyst to consider how errors in that information might influence vehicle safety. Additionally, the model needs to consider other road users in the context of the *ego vehicle's* safety, and potentially the influence that the *ego vehicle's* behaviour might have on other road users [17].

2.2. What is Driving?

Those of us who are qualified and have been driving for a period of time will likely take the task of driving for granted. We understand what it means to drive a car, but would probably find it difficult to articulate each control action and concept used. To explore the notion of driving and to inform how automation might change the assumptions on which the MISRA VCM is based, we reviewed the driver behaviour modelling research. We combined that with a review of the literature pertaining to situational awareness to understand how automation might affect driving and hence vehicle safety.

[4]the term used by the industry to describe 'our' vehicle

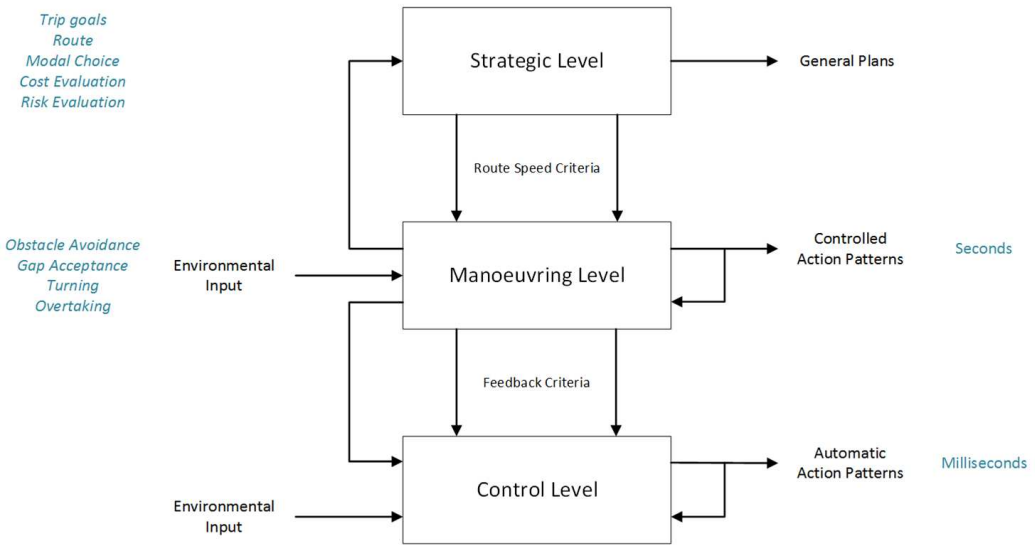

Figure 2: Michon's Hierarchical Control Model (HCM) [19]

2.2.1. Driver behaviour

Driver behaviour can be thought of as resolving the multiple possible actions (or driving related subtasks) and their effects that are presented simultaneously in a dynamically changing environment [18], and driver behaviour research can be traced back to Gibson and Crooks' 1938 research. However, it is suggested that driver behaviour research stagnated in the 1970's until in 1985 Michon published his seminal Hierarchical Control Model (HCM). The HCM (Figure 2) has three layers, (*Strategy*, *Manoeuvring* and *Control*), and Michon suggests that to be comprehensive a driver model should contain all 3 layers and provide information flow control between the layers [19]. The HCM has formed the foundation of subsequent driver conceptualisations [20], although contemporary driver models exist [21] their purpose has tended to mimic driver behaviour in a simulation context, rather than conceptualising driver behaviour in a hazard identification and analysis context.

2.2.2. Situational awareness

Fundamental to a driver's ability to safely control their vehicle, in a continually changing environment, is developing and maintaining an awareness of the objects and threats in that environment. This dynamic mental model of

the driving environment is often referred to as *situational awareness* (SA)[22]. Popular and widely cited[5], Endsley's *3 Level Model* [23] considers an individual's SA as: Level 1 SA *perception of the elements* in the environment relating to the current task, Level 2 SA *comprehension of situation* involving comprehending data from Level 1 (i.e. the significance of objects and events), and Level 3 SA *projection of future states* involving predicting the future states of the system and elements using a combination of Level 1 and 2 SA related mental models. Endsely's Model has been used in combination with Michon's Model to consider the SA needed by each hierarchical control level [24, 25], giving a concept in which the criticality of SA mental models [26] and factors affecting SA, such as distractions [22], might be considered in the context of vehicle safety.

2.3. Analysing Complex Systems

Since the 1930's analysts have used accident models to understand accidents and thus manage safety. Causal-chain or 'chain of events' models, with the *Domino Model* perhaps being the earliest example, have been used to describe the accident sequence [27]. In common with other domains, the automotive industry also uses the notion of a hazard causal-chain. With a system level *malfunction* [11] leading to a vehicle level hazard, which presents in a given *operational situation* to give rise to an accident.

Although detailed and potentially longwinded, vehicle hazard analysis has typically been a desk-based activity characterised by a systematic review of functional failure effects, energetic discussions about probable driver controllability, and large spreadsheets capturing the detail of the assumptions made. While hazard analysis remains critical to achieving functional safety and SOTIF, the continued feasibility of undertaking affective and timely hazard analysis in a highly automated and connected driving context has been bought into question [28].

Two systemic accident models have emerged in recent years: the Systems-Theoretic Accident Model and Processes (STAMP), and the Functional Resonance Accident Model (FRAM). Common to both models is the notion that accidents occur when complex systems are no longer able to cope with adaptations; either when a control system applies insufficient *constraints* (or unsafe control actions) to maintain safety (in the case of STAMP) [29], or when

[5]having >8000 citations (checked May 2020)

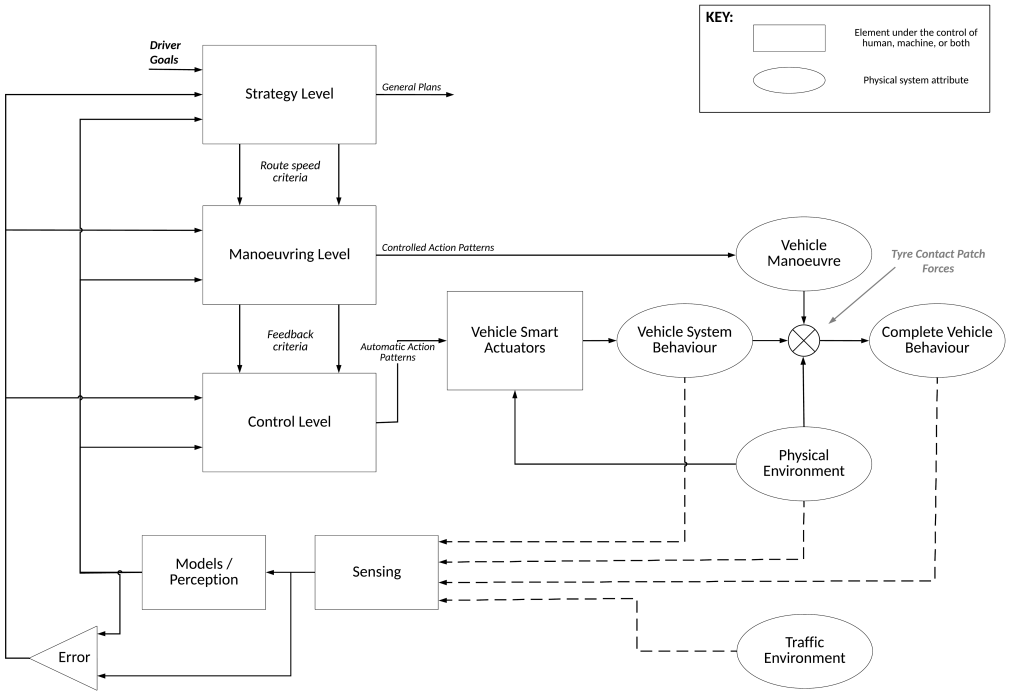

Figure 3: An Enhanced Vehicle Control Model

a control system is unable to tolerate system *variances* (in the case of FRAM) [30]. STAMP has gained traction as an alternative or complementary safety analysis method to Functional Failure Analysis (FFA) or Hazard and Operability (HAZOP) studies, which are the methods more typically used in the automotive domain [31]. While the ability to consider human behaviour in hazard analysis is clearly beneficial [32], our observation is that the 'Control Structure Diagrams' created to perform such analysis are themselves complex. Therefore, could an enhanced MISRA VCM provide a simpler Control Structure Diagram for the safety analysis of HAD vehicle features?

3. An Enhanced Automotive Risk Model

The MISRA VCM (Figure 1) remains valid for vehicle systems where the driver remains an integral part of vehicle control and has utility supporting hazard analysis and risk assessments (HARA)[16]. However, once a part of the *Driver Control* element is replaced with automation, then model defi-

ciencies become apparent. The following section describes the development of a VCM enhanced to remain relevant and useful in the analysis of highly automated and connected vehicles.

3.1. Model Construction

Initially we modified the MISRA VCM by 'splitting' the *Driver Control* element between the human and machine actors, and using data-information-knowledge-wisdom pyramids [33] to represent the different information used for human and machine perception. However, having attempted to modify the model in this way, two things became apparent: Firstly, this approach simply added complexity to the diagram, which intuitively would never lead to an elegant solution. Secondly, it did highlight a stark difference between how the human driver perceived the environment and how the machine would perceive the same environment. This raised the question as to how this difference might be used to highlight potential safety concerns, particularly when control is being shared or transferred between the human and the machine.

To reduce complexity, we used Michon's HCM (Figure 2) to represent the joint control task, but could the automated functions also fit within this hierarchy? In a discussion about multi-sensor environmental perception, a perception layer model was used to describe the interface between sensors and the higher level automated driving functions [34]. Considered together, a relationship could be made between the three models allowing the enhanced representation of the *Driver Control* element to be made.

While the meaning of each MISRA VCM element is perhaps intuitive in a manual driving context, the meaning becomes less clear in a highly automated and connected vehicle context, necessitating the underlying meaning of each model element to be defined (see Section 3.2). The MISRA VCM also used solid and dotted lines without explanation (see Figure 1). We interpret the solid lines to represent physical interfaces or interactions, and the dotted lines to represent the interpretation or perception of something physical. We then reviewed the model from a psychological view point. The result of which was the inclusion of a mechanism that represented updating of agent prior knowledge (mental models), and future state predictions, based on sensory perception [35]; effectively, the notion of obtaining and maintaining SA. This is represented in the enhanced model by a comparator. Combining these concepts gave rise to the Enhanced VCM (Figure 3).

3.2. Elements of the Model Explained

Navigating the model (Figure 3) from the top left, the first input is *Driver Goal*. These are the driver's[6] high-level objectives (e.g. drive to work, take the kids to school, or just go for a ride in the country). Achieving these goals requires strategic planning, represented by the *Strategy Level* box. These routing / planning type decisions will be influenced by information (e.g. the current *Traffic Environment*) and any goal related constraints (e.g. to arrive by a particular time), and typically occur over a long time-frame which does not require a real-time response [36]. *Route speed criteria* represents interlayer targets information from the *Strategic Level* influencing the *Manoeuvring Level*. For example the level of urgency, as a leisurely drive may become faster paced as traffic adversely affects progress.

Moving anti-clockwise around the model, the *Manoeuvring Level* represents the monitoring and regulating tasks, like negotiating a junction or determining the appropriate speed for the conditions. These will be rule based real-time tasks that typically last a few seconds [36], be predominately data driven and largely constrained by the characteristics of the given situation, and be in support of the goals set by the *Strategy Level*.

In Michon's HCM the *Manoeuvring Level* has two outputs – *Controlled Action Patterns* and *Feedback Criteria*. The literature doesn't convey the intention of these two outputs. We postulate that the *Controlled Action Patterns* represent the rule-based [37] behaviour needed to conduct the intended manoeuvre, while *Feedback Criteria* represents the information needed by the *Control Level* to successfully undertake the desired manoeuvre. For example, knowing that on a cold day the road might be slippery so choosing to limit the magnitude of steering and braking inputs.

Similar to Michon's HCM, the *Manoeuvring Layer* receives environmental information, but via the *Models / Perception* and *Error* elements. Also, we postulate that the *Manoeuvring Layer* would receive and make decisions based on feedback received from the *Control Layer*. The final output from the *Manoeuvring Layer* is a feedback path to the *Strategy Level*. For example, information about the expected arrival time of the current journey.

Below the *Manoeuvring Level* is the *Control Level*, which contains the low level driving behaviours that are largely skill-based [37], automatic and occurring in the millisecond time-frame [36]. Example *Control Level* tasks

[6]or vehicle occupants in a fully automated driving context

include steering, braking and accelerating. Being the basal level in the hierarchy, the *Control Level* has only one output; the *Automatic Action Patterns* that comprise the control actions to the vehicle control system, which we refer to as the *Vehicle Smart Actuators*.

Like the other levels, the *Control Level* has inputs that will modify its behaviour. In Michon's HCM these were the environment, *Automatic Action Patterns* feedback and *Feedback Criteria* from the *Manoeuvring Level*. We suggest that environmental inputs, both about the physical environment (e.g. carriageway edge, air temperature) and the *Complete Vehicle Behaviour* (e.g. lateral and longitudinal acceleration), and *Automatic Action Patterns* feedback (e.g. steering torque, display information) will come via the *Models / Perception* and *Sensing* route.

The *Sensing* block represents both the human senses and the machine sensors used to collect *Vehicle System Behaviour*, *Complete Vehicle Behaviour*, *Physical Environment*, and *Traffic Environment* data. For the human this might be sight and the vestibular system, for the machine this might be RADAR, LiDAR and cameras. The *Models / Perception* block is included to represent the idea of the controlling agent (i.e. human, automation, or both) obtaining and maintaining SA within the model. The *Model / Perception* block represents both the model of the environment in which the vehicle is operating, and the perception of the vehicle's behaviour within that environment. For example, the model might include information about stationary objects in the vehicle's physical environment or data regarding the current vehicle speed. We postulate that these models will be developed from information inferred from sensory data via the *Sensing* block, and updated accordingly by new data received.

From a control perspective the path from physical system attributes (*Vehicle System Behaviour, Complete System Behaviour, Physical Environment, Traffic Environment*) through *Sensing* and *Models / Perception* can act as a control path for both feedback (or compensatory) control or feed forward control [36]. We postulate that large errors between the current *Models / Perception* and new data being received via the *Sensing* block will potentially influence those blocks and drive changes in cognition for the human agent. The threshold at which this influence occurs might affect safety. For example, the human might take back control prematurely because they perceive an issue occurring, or they may continue to use the automated system in inappropriate circumstances because they are unaware of inbuilt limitations [38]. We have represented this notion by including an *Error* block having

feedback paths to the *Control Level*, *Manoeuvring Level* and *Strategy Level* blocks.

The last part of the enhanced model is the 'plant model'. Although representing a road vehicle, we envisage that other plant models (e.g. aircraft, ship, off-road vehicle) could be substituted. The vehicle plant model comprises the *Tyre Contact Patch* and the physical system attributes that influence and are influenced by the *Tyre Contract Patch*. This remains largely unchanged from the original model (Figure 1). The *Tyre Contact Patch* is the small area where the tyre and road surface are in physical contact, with an amount of slip generating the friction needed for the tyre to apply a force to the road surface, either laterally, longitudinally or both. The physical system attributes of *Physical Environment, Vehicle System Behaviour* and *Vehicle Manoeuvre* all influencing the forces being applied to the road by the tyre, while the *Complete Vehicle Behaviour* is influenced by the forces that result from the tyre-road interaction.

The *Vehicle Manoeuvre* represents the manoeuvre currently being carried out by the vehicle and will influence how the *Vehicle System Behaviour*, applied at the *Tyre Contact Patch*, translates to the *Complete Vehicle Behaviour*. For example, entering a corner too quickly may lead to excessive side-slip resulting in vehicle under-steer. The *Vehicle System Behaviour* is the vehicle level behaviour that occurs in response to system level changes made by the smart actuators. For example, positive or negative torque being applied to the vehicle's driven wheels. Next, the *Physical Environment* represents the environment in which the vehicle is being operated (e.g. weather). This will influence how the *Vehicle System Behaviour* translates to *Complete Vehicle Behaviour*, but also environmental characteristics like temperature will also influence the *Vehicle System Behaviour*. Finally *Complete Vehicle Behaviour* represents the physical vehicle response, which can be described using the 6 degrees of freedom rigid body model.

4. Evaluating the Enhanced Vehicle Control Model

By enhancing the MISRA VCM we aim to develop a model and analysis method that supports automotive safety practitioners undertaking hazard analyses [10, 11]. Before progressing further it is prudent to carry out a preliminary evaluation of the model. This preliminary evaluation will take ADAS features, having increasing levels of automation, and attempt to model those systems using only the elements available in the enhanced model. By

using ADAS features having progressively more authority over the DTT, and hence vehicle safety, the model's utility across different levels of automation can be assessed. Also the identification of artefacts common across the automation levels, and that are critical to safety, will help shape the supporting analysis method, which is the subject of future research.

4.1. Evaluation Method

To begin evaluating the Enhanced VCM required us to first define some controlling functionality and to allocate that to the *Strategy, Manoeuvring* and *Control* Levels. For this we turned to the Hierarchical Task Analysis of Driving (HTAoD) taxonomy [39]. This taxonomy defines four categories of driving task: "Perform basic control tasks", "Perform operational driving tasks", "Perform tactical driving tasks" and "Perform strategic driving tasks". We've assigned "Perform basic control tasks" to the *Control Level*, "Perform operational driving tasks" and "Perform tactical driving tasks" to the *Manoeuvring Level*, and "Perform strategic driving tasks" to the *Strategic level*. The full HTAoD contains as many as six levels of abstraction for each category. For our evaluation we chose a single level of abstraction (as shown in Figure 4) to achieve the compromise between learning from the detail, while avoiding becoming swamped by complexity.

For each task comprising vehicle control, the human or machine agents can be designated as either doing, monitoring, or being responsible for the safety of that task. Where "Do" refers to the agent undertaking the task, "Monitor" represents the agent who is able to check the progress of the activity under way, and "Safety" represents the agent who is deemed to be responsible for overall safety. The current insurance and regulatory paradigms would suggest that the responsible agent is the human in all cases. However, in an attempt to learn more from the evaluation, we have taken a more pragmatic view. That is, to consider "safety responsibility" as the agent having the potential to identify that an unsafe situation is developing and to take the appropriate mitigating action[7].

With the HTAoD tasks in mind we then considered the elements of the Enhanced VCM, looking for clues as to what the model could tell us about the safety of the different ADAS technologies chosen. We discuss the Enhanced

[7]The recent Law Commission review of the laws related to autonomous driving in the UK contains the notion of a "user in charge" suggesting that the concept of a responsible agent is likely to remain important [40].

Perform pre-driving tasks	Perform pre-operative procedures	Start the vehicle						
Perform basic control tasks	Pull away from standstill	Perform steering actions	Control vehicle speed	Decrease vehicle speed	Undertake directional control	Negotiate bends	Negotiate gradients	Reverse the vehicle
Perform operational driving tasks	Emerge into traffic from side road	Follow other vehicles	Overtake other moving vehicles	Approach junctions	Deal with junctions	Deal with crossings	Leave junction (crossing)	
Perform tactical driving tasks	Deal with different road types / classifications	Deal with roadway related hazards	React to other traffic	Perform emergency manoeuvres				
Perform strategic driving tasks	Perform surveillance	Perform navigation	Comply with rules	Respond to environmental conditions	Perform IAM[1] system of car control	Exhibit vehicle / mechanical sympathy	Exhibit driver attitude / deportment	
Perform post-driving tasks	Park the vehicle	Make the vehicle safe	Leave the vehicle					

[1] IAM - Institute of Advanced Motorists

Figure 4: Hierarchical Task Analysis of Driving (HTAoD) taxonomy [39]

VCM in the context of Adaptive Cruise Control (ACC) (Section 4.1.1), ACC with Lane Centring (Section 4.1.2) and Traffic Jam Assist (Section 4.1.3) below.

*4.1.1. Adaptive Cruise Control (ACC) (*SAE Level 1*)*

ACC is categorised as an SAE Level 1 [9] automation system because, when activated by the driver, the vehicle system takes responsibility for longitudinal vehicle control (i.e. accelerating and braking). This is achieved either by maintaining the speed set by the driver, or by reducing vehicle speed to maintain a set distance (referred to as *headway*) to the vehicle in front. Early ACC systems had limited capability and so were typically sold as *assistance system*. Today's systems are more capable, with the ability to reliably reject non-traffic targets and having sufficient authority over the vehicle's control systems to bring the vehicle to a complete stop.

The matrix in Figure 5 has been coloured considering the DDT influenced by the introduction of ACC. With ACC functionality controlling vehicle speed to a value set by the driver it is fair to assume that the "Control Vehicle Speed" and "Negotiate Gradients" HTAoD task will be influenced by ACC. Additionally, with functionality to maintain the *headway* to the vehicle in front, the feature must also be capable of "Decreasing Vehicle Speed" and "Following Other Vehicles." Our ACC vehicle feature also includes the capability to brake the vehicle to a stand still, so the task of "Pulling Away From Standstill" also warrants consideration.

Reflecting on ACC functionality in relation to the control layers (Figure 3) it is reasonable to expect the responsibility for all *Strategy Level* tasks to remain with the human agent. The same is true of *Manoeuvring Level*

tasks, with the exception of "Follow other vehicles" which does come under the control of the machine agent while ACC is active.

For *Control Level* tasks there is a greater responsibility split. When considering the agents' responsibilities, the "Do" aspects of the "Control Vehicle Speed" and "Negotiate Gradients" tasks can be coloured green as they represent tasks covered by standard cruise control today. We have also chosen to colour the "Monitor" responsibility for these tasks green. Being an *assistance system* one could argue that all ACC monitoring tasks should be blue. However, because the monitoring of these tasks requires only simple closed loop control, which is unlikely to be adversely affected by external factors, we argue that the monitoring work-load for the human driver would be small.

With ACC having the capability to decrease vehicle speed and to follow other vehicles the "Do" has been coloured green to designate that the machine agent is responsible. The categorisation for "Monitor" is less clear. One can quickly conceive of driving scenarios where "Follow other vehicles" cannot be fully monitored by the machine. For example, if ACC is maintaining the *headway* to the vehicle in front, when another vehicle cuts into that gap and brakes, ACC may require the driver to intervene. Typically this occurs because the level of braking force needed is greater than ACC is authorised to command from the brake system. It would also be fair to conclude that had this scenario occurred during manual driving, the human driver would have reacted to the developing situation more quickly. Thus needing a less aggressive braking response because their perception of the traffic environment is greater – being able to both perceive objects in the environment (SA Level 1), but also to project to a future state (SA Level 3). When considering the responsibility for monitoring the "Decrease vehicle speed" similar logic is applied, consequently "Monitor" is coloured blue.

Uniquely the "Do" responsibility for "Pulling Away from Standstill" has been coloured blue. This is because our ACC vehicle feature requires the driver to press the RESUME button, to re-activate ACC, once the vehicle is stationary. ACC typically incorporates this behaviour for two reasons: Firstly, to avoid a scenario where a pedestrian, with a poor RADAR cross-section, goes undetected by ACC. Secondly, to avoid the potential hazard of the driver turning their attention to a non-driving task while the vehicle is stationary being totally unprepared when the vehicle does pull away. Following the same logic that the correct behaviour of the "Pull away from standstill" task can be adversely affected by what is going on around the

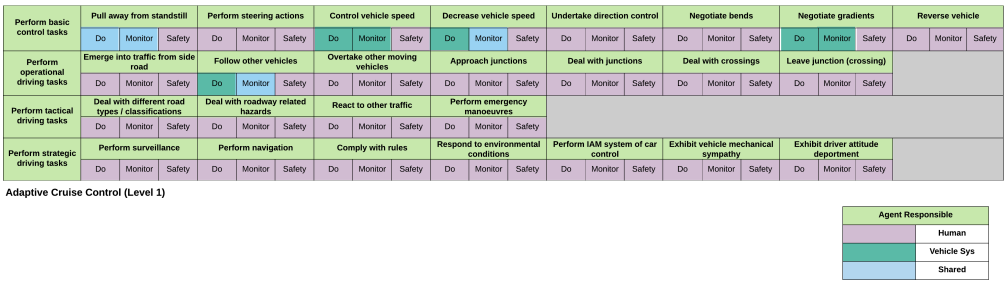

Figure 5: HTAoD Tasks with Responsibility Designation for ACC (SAE Level 1)

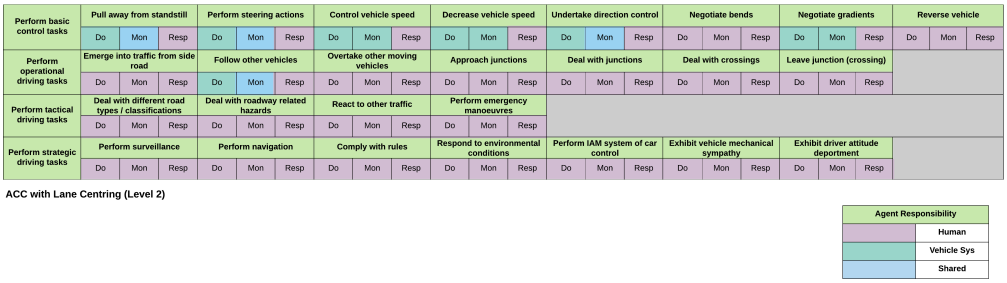

Figure 6: HTAoD Tasks with Responsibility Designation for ACC with Lane Centring (SAE Level 2)

vehicle, "Monitor" has been designated as a shared task also.

4.1.2. ACC with Lane Centring (SAE Level 2)

ACC with Lane Centring is an evolution of ACC having increased capability to support the driver by maintaining the vehicle's central position in lane. While ACC is active, lane centring is achieved by the system continuously applying torque to the steering rack. While ACC with Lane Centring is active it is providing both longitudinal and lateral control simultaneously, so is categorised as a Level 2 system by the SAE taxonomy [9].

Like ACC, all *Strategy Level* and all but one *Manoeuvring Level* task remains under the control of the driver while the feature is active. The only *Manoeuvring Level* task that we consider to be a shared task is 'Follow Other Vehicles'. Intuitively one might expect to see a *Manoeuvring Level* steering task included in the HTAoD taxonomy, but no comparable steering task appears at the *Manoeuvring Level*. Instead it is an unconscious *Control*

Level task, buried in the application of a given manoeuvre.

Our ACC with Lane Centring vehicle feature is able to detect the driver's hands on the steering wheel, and will warn and ultimately disable the system if the driver removes their hands from the steering wheel for a significant period of time. Given this (near) constant engagement in the steering task the responsibility for both "Perform Steering Actions" and "Undertake Direction Control" have been assigned assuming that: the vehicle system will "Do" the task, the human driver and the machine will share the "Monitor" task, while the human driver is responsible for "Safety". The similar task of "Negotiate Bends" is considered to remain the responsibility of the human driver under all conditions; given the relatively low level of steering authority that the system has (i.e. correctly navigating anything other than a gentle Motorway curve would require driver intervention).

The notion of the human driver correctly identifying the conditions in which to enable or disable ACC with Lane Centring does identify a task, not included in the HTAoD, namely a "Use Automation Appropriately" task. Considering this new task in the context of the Enhanced VCM we postulate that the "Use Automation Appropriately" task would be undertaken at the *Strategy Level* by the human driver. For the human driver to carry out this task effectively they not only rely on the correct perception of the *Traffic* and *Physical Environments*, but they also need to understand the capabilities and limitation of the automation being used. We postulate that the driver will have feature behaviour mental models stored within the *Models / Perception* element that will have developed over time through using the feature, experimentation, and possibly through reading the Driver's Handbook! Consequently, the accuracy of the driver's ACC with Lane Centring mental model, regarding capability and appropriateness of use [41], will be largely dependent on when and where the driver used the feature previously, and how the feature appeared to respond. For example, a RADAR sensor blocked with packed snow could adversely affect longitudinal control if not detected. To maintain safety the driver would need *awareness* [42] that the systems had lost capability, so that they could cancel ACC with Lane Centring and resume manual control before the loss of capability led to potentially hazardous behaviour. Figure 7 uses the Enhanced Model to explore this scenario where fog or falling snow is affecting the automation's ability to correctly perceive other vehicles and lane markings.

ACC with Lane Centring raises further questions about how the human driver's awareness of the driving task and their perception of the surroundings

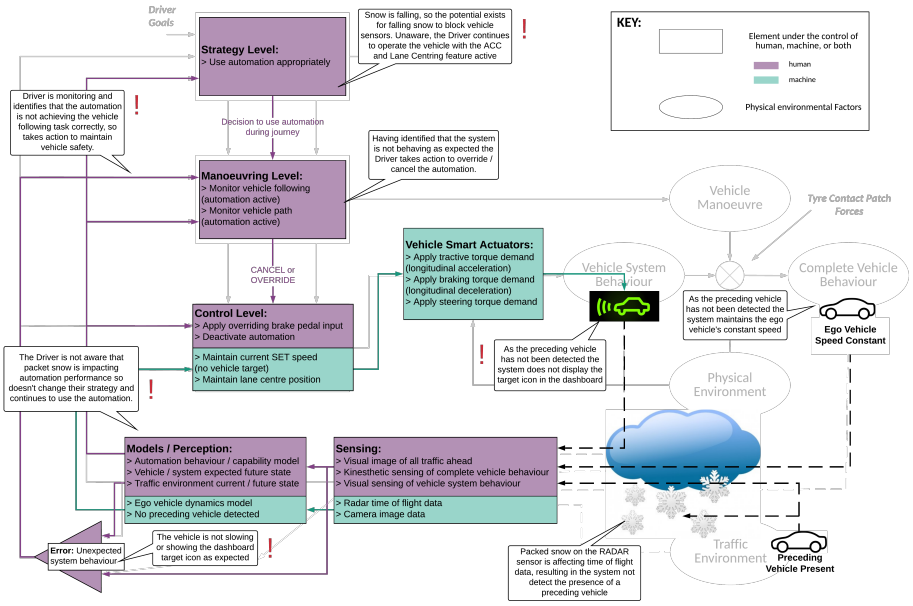

Figure 7: Using ACC with Lane Centring (SAE Level 2) with the Physical Environment Influencing Automation

might change. Although both longitudinal and lateral control are considered to be *Control Level* tasks, it is suggested that whether longitudinal or lateral vehicle control is automated has an effect on the human driver's response, engagement with automation, and ability to regain control; with the suggestion being that the driver will focus less far ahead of their own vehicle when lateral control is automated compared to longitudinal control [2]. A situation that is probably exacerbated by a less engaged and drowsy driver. Figure 8 uses the Enhanced Model to capture the idea of a loss of driver attentiveness.

4.1.3. Traffic Jam Assist (SAE Level 3)

The feature Traffic Jam Assist (TJA) is a further evolution of ACC with Lane Centring, giving the driver a near *"hands and feet off"* driving experience within a very constrained operating scenario. Typically, the Operational Design Domain (ODD) specifies that the vehicle is operated at relatively low speeds (e.g. below 65 km/h) in congested traffic. Once activated TJA will control vehicle steering, acceleration and braking to maintain the vehicle's position in lane and within the traffic queue. Once the driver has engaged TJA they are considered to have relinquished control to the system, however

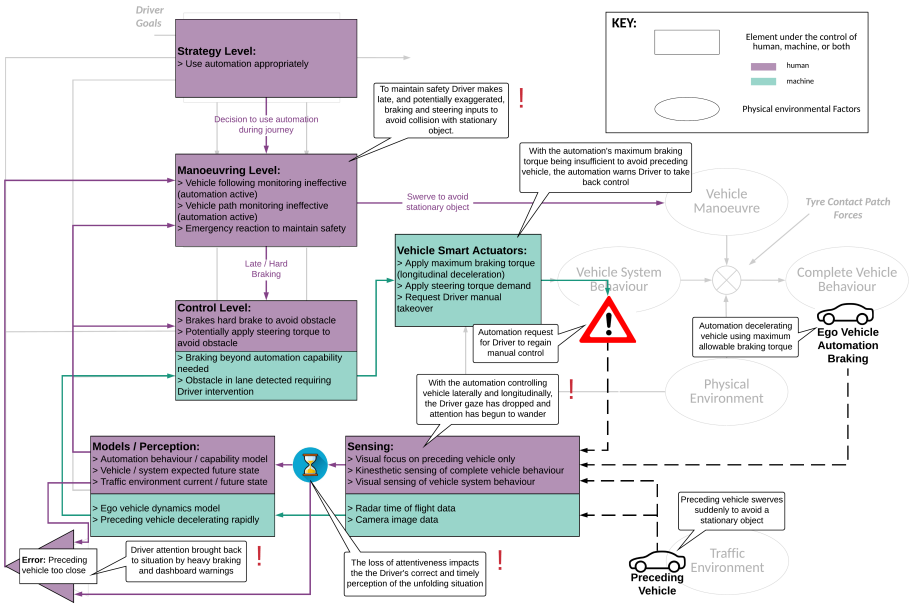

Figure 8: ACC with Lane Centring (SAE Level 2), a stationary obstruction and an inattentive driver

the driver must remain vigilant and intervene to maintain safety if circumstances require. For this reason the system is considered to be a Level 3 system [9].

The SAE taxonomy defines Level 3 as a system having full vehicle control in a given context, but without the capability to maintain safety in that same context. Given the safety concerns this raises, a "true" Level 3 system would likely be considered unsuitable for production. Instead the system would need to maintain some level of availability, to enable the driver to regain manual control successfully. For example, if the system fails to confirm that the return to manual control has been successful then it will switch on the vehicle's hazard lights and bring the vehicle to a controlled stop in lane.

Considering the HTAoD in the context of TJA, the increased influence that automation has over vehicle control becomes evident; with only the "Undertake direction control", "Negotiate Bends" and "Reverse Vehicle" *Control Level* tasks being unaffected by the feature. Of those *Control Level* tasks influenced by TJA, the "Do," "Monitor," and "Safety" attribute for each task have been rated as "vehicle system" (green), "vehicle system" (green), and "shared" (blue) respectively.

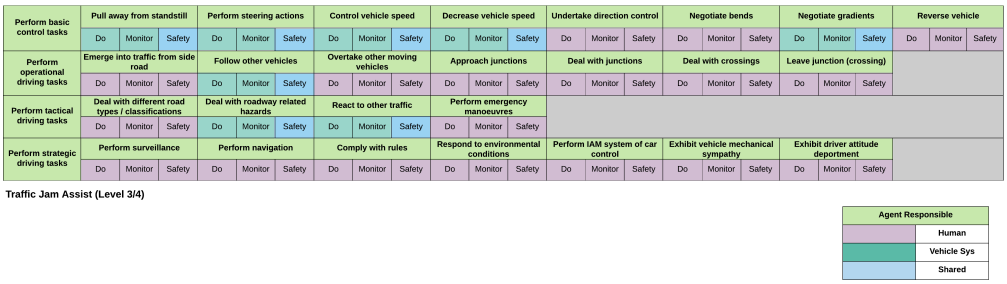

Figure 9: HTAoD Tasks with Responsibility Designation for Traffic Jam Assist (Level 3)

The influence that TJA has over the *Manoeuvring Level* tasks is still quite limited, with "Deal with Road Related Hazards" and "React to Other Traffic" being influenced in addition to "Follow Other Vehicles" which was influenced by the vehicle features discussed previously (see Sections 4.1.1 and 4.1.2). Our assessment of TJA suggests that 8 out of 26 task groups considered will be affected by the feature, with the automated tasks allowing the driver to effectively remove themselves from the vehicle control loop. In such cases how does the driver maintain sufficient SA to intervene should a situation affecting safety arise? And if the driver has relinquished control to the automation, will they be capable of delivering a measured and timely response if the situation requires it? Long standing human factors thinking would suggest that once out of the control loop humans are not good at monitoring what the control is doing [43] and more recent specific research into the resumption of steering control would suggest that drivers are slower to respond to situations once out of the loop, and when the driver's response does come then its magnitude may be too large or even erratic [13].

From a controllability perspective the perception and SA models required by the driver are complex. For TJA the human driver needs to maintain SA of both the *Traffic Environment* and *Complete Vehicle Behaviour*. However, to achieve that requires good system behaviour mental models, such that they can correctly judge when to intervene to maintain safety. Ultimately, a vehicle feature's capability, and ability to correctly sense its environment, is a function of the sensor suite. While writing this paper we looked at manufacturers' marketing material available and found similar sounding vehicle features have quite different sensor sets and hence capabilities. For example, Audi offers TJA features on its Q2 and Q7 models. However, with its

richer sensor set, the Q7 vehicle has the ability to follow the preceding vehicle convoy around a stationary object (e.g. the marketing video shows the vehicle manoeuvring around a stranded vehicle that is partially on the hard-shoulder and partially in the 'live' lane) [44] whereas the Q2 does not have this capability. In addition to the missing *Strategy Level* "Use Automation Appropriately" driving task discussed in Section 4.1.2 there is perhaps then the need for a "Monitor Automation" *Manoeuvring Level* driving task as well [45]. Although as seen with TJA, what this task demands is dependent on the capability of the automation.

5. Discussion

5.1. The Enhanced Vehicle Risk Model

Fundamental to the safe operation of a vehicle is having and maintaining SA of the ever-changing environment, with mental models being critical to maintaining SA [26]. Reflecting on this in the context of the MISRA VCM (Figure 1) highlights the need to model human cognition within the Enhanced VCM; particularly the potentially stark difference in environmental perception capability between the human and the machine. If the perception capability of the automation is less than that of the human driver, then we suggest that the resultant system behaviour could be unexpected, unwanted or result in the human developing an incorrect mental model of the automation's actual behaviour. The potential for either the human being *surprised* by the automation, or the automation responding more slowly or incorrectly compared to the human, led us to add perception and error blocks to the original diagram in addition to a hierarchical control model.

5.2. Preliminary Evaluation

The Enhanced VCM has been considered in the context of three use cases to give a preliminary evaluation of its utility. Three vehicle features (ACC, ACC with Lane Centring and TJA), having increasing levels of automation authority where chosen for this evaluation.

Considering the Follow Other Vehicle task, in the context of ACC, highlighted the potential affect of differences in perception (see Section 5.1) for the cut-in scenario. In this scenario the automation is unable to perceive a vehicle cutting in from an adjacent lane, so will not brake until the 'cut in' vehicle is well into the *ego vehicle's* own lane. However, with the driver still in the control loop and situationally aware, they will typically react quickly

to other visual cues and cancel ACC well before the other vehicle encroaches into their lane.

The analysis of ACC with Lane Centring uncovered a new *Strategic Level* driver task of "Use Automation Appropriately". Due to sensing capabilities and the level of authority afforded to the vehicle feature (e.g. amount of steering and braking torque that the system is allowed to apply to the vehicle smart actuators) the driver will need to understand the capabilities of the feature and only operate the system when it is safe and appropriate to do so. To "Use Automation Appropriately" and to successfully intervene when needed, requires the driver to not only be situationally aware, but also to have knowledge of the automation's capability [41].

Giving the driver the new task of "Monitor Automation" is perhaps an obvious consequence of adding automation to driving. However, discussing TJA in the context of the Enhanced VCM does highlight how the "Monitor Automation" task could become quite complex for SAE Levels 3 and 4 automation; particularly if the driver moves between vehicles, having similarly named HAD features, but with very different system capabilities.

5.3. Further Evaluations

Our initial evaluation has demonstrated that HAD features can be discussed in the context of the Enhanced VCM (Figure 3). Having "tested" the model's applicability in the broadest sense, further evaluations are planned to further explore the model's applicability, and to develop an analysis method that will support automotive hazard analyses.

5.3.1. Cooperation

A cognitive system is defined as *"a system that can modify its behaviour on the basis of experience so as to achieve specific anti-entropic ends"*. As such, the activity of driving can be viewed as a joint cognitive system (JCS); as a combination of actions are required, within the context of sometimes unpredictable and dynamic environment [46]. The three HAD features (Sections 4.1.1 to 4.1.3) previously discussed highlighted the importance of the human machine interface in maintaining safety. However, until this point we have only made generalisations about how SA, perception and an understanding of automation performance might impact safety. When considering HAD safe operation and the *ego vehicle's* behaviour in relation to that of other vehicles, the importance of the human and machine agents cooperating to achieve timely and effective control responses is evident; particularly regarding the

correct application of evasive manoeuvres. However, with the expectation being that increased automation will detrimentally impact a driver's SA and reaction time (time to engage) [2], while misunderstandings regarding the automation's capability might result in the automation issuing more take-over requests, we feel it important to add a temporal dimension to the Enhanced VCM. But what form should this temporal dimension take?

The Contextual Control Model (COCOM) is a cyclical model of human action, with *competencies* being the possible actions that can be taken, *control* being the way in which *competencies* are chosen, while *constructs* describe the context in which the action is carried out [46]. Although contemporary research now suggests that the human cognition actually uses a process of *predictive processing* [35], that is continuously predicting its own sensory inputs and acting upon the predictive error, the *competency, control, constructs* loop is probably still a useful model. An extension of COCOM is the Enhanced Control Model (ECOM). This model incorporates multiple control loop layers, to reflect the many layers of activities normally taking place concurrently within a JCS. By considering how control is lost, regained and performance changed, the suggestion is that ECOM provides a useful framework from which to explore the effects of automation on JCS [46]. We therefore plan to incorporate the ECOM framework into the Enhanced VCM to see if the resulting model does provide insight into the identification of hazards associated with the temporal nature of control and the impact of automation. This is the subject of our future research.

5.3.2. Risk Analysis Methods

Our future research also involves developing an analysis method to accompany the Enhanced VCM. For this we will consider the systemic analysis techniques of FRAM and STPA; to identify and evaluate whether it is appropriate to incorporate such techniques into our method. Although potentially time consuming, FRAM has been identified as an enabling technique for identifying interactions between system functions that are critical, and the system dynamics that emerge given variability in those reactions [47]. Furthermore, when combined with Rasmussen's Abstraction Hierarchy, FRAM's utility in analysing multi-layer functionality has been demonstrated [48]. The STPA analysis technique [49] is becoming the *de facto* safety analysis method used by the automotive ADAS development community. However, evidence would

suggest that the models produced are complex[8].

Taking these ideas further, could the Enhanced VCM be used as a framework from which to analysis HAD functional hierarchies, systemic interactions and variances? Furthermore, given the popularity of STPA within the automotive domain could the Enhanced VCM be used to minimise model complex when STPA is used in an automotive context? These ideas will be the subject of our future research.

5.3.3. The Task of Driving

The HTAoD taxonomy provided a useful prompt when considering the dynamic driving task in the context of increasing automation. Particularly, what tasks constituted *Driver Control* (Figure 1) in any given scenario, and where each task should reside within the *Strategy, Manoeuvring* and *Control Levels* (Figure 3). However, being a taxonomy for manual driving it does lack the tasks associated with vehicle automation. As identified in Section 4 this could require the inclusion of the *Strategy Level* task of "Use Automation Appropriately" and *Manoeuvring Level* tasks of "Monitor Automation" and "Resume Direction Control". Therefore, any automation analysis method that incorporates the HTAoD taxonomy will need to be expanded to include these new tasks.

With contemporary methods like FRAM and STPA analysing a system's functional, a taxonomy that is functional rather than task based would probably be more appropriate. Indeed, recent literature [50, 51] does describe HAD features, including Traffic Jam Pilot and Highway Pilot, using a generic functional hierarchy. The identification of a suitable driving activity taxonomy, be it task or functional based, for our analysis method will be the subject of further research.

6. Conclusions

Within this paper we have presented an Enhanced VCM, which is based on the MISRA Control System View of the Vehicle model, but that incorporates contemporary research concepts to extend the model's utility in an HAD context. Although we have presented the enhanced model purely from

[8]The Control Structure Diagram presented in *Functional Safety Assessment of an Automated Lane Centering System* contains 26 individual system elements [31].

the perspective of automotive based automation, generic human factors concepts have been used. Therefore, we expect these concepts and our conceptual model to work equally well with plant models in other operating contexts. We have described the intent of the model's elements and used three ADAS vehicle features (i.e. ACC, ACC with Lane Centring and TJA), having progressively higher authority over vehicle control, to elaborate the meaning behind each model element. Then the HTAoD taxonomy has been used to focus on driving tasks where a shared responsibility, and hence potential hazard cause exists. The Enhanced VCM has allowed us to discuss potential hazards caused by differing perception levels between the human and the machine. However, without the ability to reason about the temporal nature of that interaction, we expect potential hazard causes to remain undiscovered. For the Enhanced VCM to become a useful addition to the automotive safety analyst's 'tool box' not only does it need to include a temporal element, but it also requires an accompanying method. These aspects are the focus of our future research.

7. References

[1] Motor Industry Software Reliability Association . Development guidelines for vehicle based software. Guideline; MISRA; 1994. URL: www.misra.org.uk.

[2] Carsten O, Lai F, Barnard Y, Jamson H, Merat N. Control task substitution in semiautomated driving: Does it matter what aspects are automated? Human Factors: The Journal of the Human Factors and Ergonomics Society 2012;.

[3] Stevens A, Brusque C, Krems J. Driver adaptation to information and assistance systems. IET Publication 2013;.

[4] Banks VA, Eriksson A, O'Donoghue J, Stanton NA. Is partially automated driving a bad idea? Observations from an on-road study. Applied Ergonomics 2018;68:138–45. URL: http://www.sciencedirect.com/science/article/pii/S0003687017302594.

[5] Motor Industry Software Reliability Association . Guidelines for safety analysis of vehicle based programmable systems. Guideline; MISRA; 2007. URL: www.misra.org.uk.

[6] World Health Organization . Road traffic injuries. 2017. URL: http://www.who.int/mediacentre/factsheets/fs358/en/; [accessed on: 19-09-2019].

[7] Liu P, Wang L, Vincent C. Self-driving vehicles against human drivers: Equal safety is far from enough. J Exp Psychol Appl 2020;URL: https://www.ncbi.nlm.nih.gov/pubmed/32202821. doi:10.1037/xap0000267.

[8] Koopman P, Ferrell U, Fratrik F, Wagner M. A safety standard approach for fully autonomous vehicles. In: SAFEComp. Computer Safety, Reliability, and Security; Springer International Publishing. ISBN 978-3-030-26250-1; 2019, p. 326–32.

[9] Society of Automotive Engineers . Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. Guideline SAE J3016; Society of Automotive Engineers; 2018.

[10] The International Organization for Standardization . Road vehicles – Safety of the intended functionality. Publicly Available Specification ISO/PAS 21448; ISO; 2019.

[11] The International Organization for Standardization . ISO 26262: Road vehicles – Functional safety. International Standard; ISO; 2018.

[12] UNECE . Vienna convention on road traffic. Tech. Rep.; United Nations Economic and Social Council; 1968.

[13] Louw T, Kountouriotis G, Carsten O, Merat N. Driver distraction during vehicle automation: how does driver engagement affect resumption of control? 4th Driver Distraction and Inattention Conference 2015;.

[14] Louw T, Merat N, Jamson H. Engaging with highly automated driving: To be or not to be in the loop? Proceedings of the 8th International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design 2015;.

[15] Merat N, Jamson AH. Is drivers' situational awareness influenced by a fully automated driving scenario? Human Factors, Security and Safety 2009;.

[16] Monkhouse H, Habli I, McDermid J. The notion of controllability in an autonomous vehicle context. CARS 2015;.

[17] Merat N, Lee YM, Markkula G, Uttley J, Camara F, Fox C, et al. How Do We Study Pedestrian Interaction with Automated Vehicles? Preliminary Findings from the European interACT Project. In: Meyer G, Beiker S, editors. Road Vehicle Automation 6. Road Vehicle Automation 6; Springer International Publishing. ISBN 978-3-030-22933-7; 2019, p. 21–33.

[18] Da Lio M, Mazzalai A, Gurney K, Saroldi A. Biologically guided driver modeling: the stop behavior of human car drivers. IEEE Transactions on Intelligent Transportation Systems 2018;19(8):2454–69. doi:10.1109/tits.2017.2751526.

[19] Michon JA. A critical view of driver behavior models: What do we know, what should we do? Human Behavior and Traffic Safety 1985;:485–524doi:10.1007/978-1-4613-2173-6-19.

[20] Lützenberger M. A Driver's Mind; book section Chapter 10. Advances in Data Mining and Database Management; IGI Global. ISBN 9781466649200; 2014, p. 182–205. doi:10.4018/978-1-4666-4920-0.ch010.

[21] Peters B, Nilsson L. Modelling Driver Behaviour In Automotive Environments; chap. 5 – Modelling the Driver in Control. Springer London; 2007, p. 85 – 104.

[22] Strayer DL, Fisher DL. Spider: A framework for understanding driver distraction. Human Factors 2016;58(1):5–12. doi:10.1177/0018720815619074.

[23] Endsley MR. Toward a theory of situation awareness in dynamic systems. Human Factors 1995;37(1):32–64. doi:10.1518/001872095779049543.

[24] Matthews M, Bryant D, Webb R, Harbluk J. Model for situation awareness and driving: Application to analysis and research for intelligent transportation systems. Transportation Research Record: Journal of the Transportation Research Board 2001;1779:26–32. doi:10.3141/1779-04.

[25] J Ward Nicholas . Automation of task processes: An example of intelligent transportation systems. Human Factors and Ergonomics in Manufacturing & Service Industries 2000;10(4):395–408. doi:10.1002/1520-6564(200023).

[26] Salmon PM, Stanton NA, Walker GH, Baber C, Jenkins DP, McMaster R, et al. What really is going on? Review of situation awareness models for individuals and teams. Theoretical Issues in Ergonomics Science 2008;9(4):297–323. doi:10.1080/14639220701561775.

[27] Toft Y, Dell G, Klockner K, Hutton A. Models of causation: safety. Safety Institute of Australia, Tullamarine, Victoria 2012;.

[28] Monkhouse H, Habli I, Mcdermid J, Khastgir S, Dhadyalla G. Why functional safety experts worry about vehicle systems having greater autonomy. ATC 2017;.

[29] Leveson N. A new accident model for engineering safer systems. Safety Science 2004;42(4):237–70. doi:10.1016/s0925-7535(03)00047.

[30] Hollnagel E. FRAM: the Functional Resonance Analysis Method. Ashgate Publishing Ltd.; 2012.

[31] Becker C, Yount L, Rozen-Levy S, Brewer J. Functional safety assessment of an automated lane centering system. National Highway Traffic Safety Administration 2018;.

[32] Abidi Nasri S. Application of the STPA methodology to an automotive system in compliance with ISO 26262. Thesis; University of Stuttgart; 2018.

[33] Ayed SB, Trichili H, Alimi AM. Data fusion architectures: A survey and comparison. 15th International Conference on Intelligent Systems Design and Applications (ISDA) 2015;:277–82doi:10.1109/ISDA.2015.7489238.

[34] Robert Schubert MO. The role of multisensor environmental perception for automated driving. Automated Driving: safer and more efficient future 2016;:161 –82.

[35] Engström J, Bärgman J, Nilsson D, Seppelt B, Markkula G, Piccinini GB, et al. Great expectations: a predictive processing account of automobile driving. Theoretical Issues in Ergonomics Science 2017;19(2):156–94. doi:10.1080/1463922x.2017.1306148.

[36] Engström J, Hollnagel E. A General Conceptual Framework for Modelling Behavioural Effects of Driver Support Functions; book section 4. London: Springer London. ISBN 978-1-84628-618-6; 2007, p. 61–84.

[37] Rasmussen J. Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. IEEE Transactions on Systems, Man, and Cybernetics 1983;SMC-13(3):257–66. doi:10.1109/TSMC.1983.6313160.

[38] Victor TW, Tivesten E, Gustavsson P, Johansson J, Sangberg F, Ljung Aust M. Automation Expectation Mismatch: Incorrect Prediction Despite Eyes on Threat and Hands on Wheel. Human Factors 2018;60(8):1095–116. doi:10.1177/0018720818788164.

[39] Walker G, Stanton NA, Salmon PM. Human Factors in Automotive Engineering and Technology. CRC Press; 2017. ISBN 978-1-138-74725-8.

[40] Law Commission . Automated vehicles: A joint preliminary consultation paper. Tech. Rep. Consultation Paper No 240; Law Commission of England and Wales; 2018.

[41] Flemisch F, Heesen M, Hesse T, Kelsch J, Schieben A, Beller J. Towards a dynamic balance between humans and automation: authority, ability, responsibility and control in shared and cooperative control situations. Cognition, Technology & Work 2011;14(1):3–18. doi:10.1007/s10111-011-0191-6.

[42] Beller J, Heesen M, Vollrath M. Improving the driver – automation interaction: An approach using automation uncertainty. Human Factors: The Journal of the Human Factors and Ergonomics Society 2013;55(6):1130–41. doi:10.1177/0018720813482327.

[43] Bainbridge L. Ironies of automation. Automatica 1983;19(6):775–9. doi:http://dx.doi.org/10.1016/0005-1098(83)90046-8.

[44] Audi AG . Audi Q7 – Audi Traffic Jam Assist. 2015. URL: https://www.audi-technology-portal.de/en/electrics-electronics/driver-assistant-systems/audi-q7-traffic-jam-assist; [accessed on: 18-09-2019].

[45] Banks VA, Stanton NA. Analysis of driver roles: Modelling the changing role of the driver in automated driving systems using EAST. Theoretical Issues in Ergonomics Science 2017;.

[46] Hollnagel E, Wood DD. Joint Cognitive Systems – Foundations of Cognitive Systems Engineering. CRC Press; 2005.

[47] Adriaensen A, Patriarca R, Smoker A, Bergstrom J. A socio-technical analysis of functional properties in a joint cognitive system: a case study in an aircraft cockpit. Ergonomics 2019;62(12):1598–616. doi:10.1080/00140139.2019.1661527.

[48] Patriarca R, Bergström J, Di Gravio G. Defining the functional resonance analysis space: Combining Abstraction Hierarchy and FRAM. Reliability Engineering and System Safety 2017;165:34–46. doi:10.1016/j.ress.2017.03.032.

[49] Leveson NG, Thomas JP. STPA Handbook. Nancy Leveson; 2018.

[50] Wood M, Knobel C, Garbacik N, Wittmann D, Syguda S, O'Brien M, et al. Safety First for Automated Driving. Aptiv Services US; 2019.

[51] Thorn E, Kimmel S, Chaka M. A Framework for Automated Driving System Testable Cases and Scenarios. National Highway Traffic Safety Administration; 2018.